## REMARKS

Reconsideration of the above referenced application in view of the enclosed amendments and remarks is requested. Claims 61, 71, and 81 are the independent claims. This response amends claims 61, 71, and 81 to clarify what is meant by "isolated execution mode."

## ARGUMENT

The Final Office Action rejects the claims 61-90 based on 35 U.S.C. § 102(e). Applicant appreciates the Examiner's attention to the present application. However, Applicant respectfully asserts that those rejections are not well founded. In addition, to the extent that those rejections might be applied to the new claims, Applicant respectfully traverses.

35 U.S.C. § 102(e)

The Final Office Action rejects claims 61-90 under 35 U.S.C. § 102(e) as being anticipated by U.S. patent no. 6,226,749 to Marius Carloganu et al. (hereinafter "Carloganu"). To the extent that the rejections in the Final Office Action might be applied to any of the present claims, Applicant respectfully traverses.

For a valid rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (MPEP § 2131.01, quoting from Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

Carloganu pertains to an apparatus for processing "secured commands" and "non-secured commands" received from external devices. Specifically, according to Carloganu, "an application program running in an external device" sends non-secured and secured commands to "a secure processor" for execution. The secure processor "immediately executes" the non-secured commands, and the secured processor only executes secured commands if those commands pass tests for "authenticity" and "regularity." The secure processor determines which commands

are secured and which are non-secured by looking up each received command in a "command set up table." (Abstract.)

By contrast, claim 81 in the present application recites a processing system comprising a processor that supports "a normal execution mode in a ring 0 operating mode" and "an isolated execution mode in the ring 0 operating mode." In addition, claim 81 recites that the processor supports "one or more higher ring operating modes." Furthermore, the processor comprises an access checking circuit that prevents access to an isolated memory area of the processing system if the processor is not "set to operate in the isolated execution mode." In particular, the operations of the access checking circuit comprise "disallowing the transaction if [1] the transaction requests access to an isolated memory area of the processing system and [2] the processor is not set to operate in the isolated execution mode."

Carloganu says nothing about an "isolated execution mode," or a "ring 0 operating mode." Carloganu therefore cannot possible anticipate claim 81, which recites a processor that supports "an isolated execution mode in the ring 0 operating mode." Furthermore, Carloganu says nothing about any "higher ring operating modes." Carloganu therefore cannot possibly anticipate claim 81, which recites that the processor also supports "one or more higher ring operating modes."

The other pending independent claims (i.e., claims 61 and 71) include features that are the same as or similar to the features discussed above with regard to claim 81, and the dependent claims inherently include the features of their respective parent claims. Carloganu therefore does not anticipate any of the pending claims.

Moreover, as indicated above, Carloganu uses a command set up table to determine whether a command is a secured command, and then only executes secured commands if those commands pass tests for "authenticity" and "regularity." Carloganu says nothing about determining whether a command involves access to memory. Carloganu also says nothing about disallowing transactions, based on the type of memory area to be accessed and the current setting of the processor, and Applicant respectfully traverses all assertions to the contrary in the Final Office Action.

For example, the Final Office Action asserts that Carloganu discloses (at column 2, lines 35-67) disallowing a transaction based on the type of memory area to be accessed and the current setting of the processor. That assertion is incorrect. In particular, although the cited section of Carloganu may pertain to the general topic of disallowing transactions, it does not disclose that transactions are disallowed based on the type of memory area to be accessed and the current setting of the processor. Instead, that section states that commands are disallowed based on tests for "command sequence" and "command authenticity." For example, with regard to "command sequence," that section explains that commands may be "required to be executed ... in an ordered numerical sequence." With regard to "command authenticity," Carloganu explains that a "message authentication code signature value in the secured command is checked to determine of it matches the test message authentication code signature value." Carloganu does not disclose that commands are disallowed based on the type of memory area to be accessed. Carloganu does not disclose that commands are disallowed based on the current setting of the processor. Applicant therefore traverses the assertion that Carloganu discloses disallowing a transaction based on the type of memory area to be accessed and the current setting of the processor.

In addition, the claims recite numerous additional features that are not disclosed by Carloganu. For example, claim 82 recites that the access checking circuit "allows access to the isolated memory area when the processor is set to operate in the isolated execution mode" and "prevents access to the isolated memory area when the processor is not set to operate in the isolated execution mode." Claim 84 recites that the processor (a) creates an isolated memory area in the memory of the processing system, based at least in part on configuration parameters for the isolated memory area, and (b) determines whether the transaction requests access to the isolated memory area, based at least in part on (i) access information for the transaction and (ii) one or more of the configuration parameters for the isolated memory area. Claim 86 recites that (a) the processor comprises "a processor control register to store an isolated execution mode setting," and (b) the processor determines whether the processor is set to operate in the

isolated execution mode, "based at least in part on the isolated execution mode setting from the processor control register." Carloganu disclose none of these features, and Applicant respectfully traverses all assertions to the contrary in the Final Office Action.

For reasons including those set forth above, Carloganu does not anticipate any of pending claims of the present application.

Information Disclosure Statements

Applicant's prior response, filed November 23, 2004, noted that the Examiner's initials were missing from some of the references in the following Information Disclosure Statements (IDSs): (1) the IDS mailed on January 26, 2004; and (2) the IDS mailed on June 29, 2004. However, the Final Office Action did not address that point. Applicant again requests confirmation that the Examiner has considered all references listed in those IDSs.

In addition, the Final Office Action did not include a copy of the IDS that was submitted on January 13, 2005. Applicant therefore also requests confirmation that the Examiner has considered all references listed in that IDSs.

## CONCLUSION

In view of the foregoing, claims 61-90 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Prompt issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: May 17, 2005

/ Michael R. Barre /

Michael R. Barré
Registration No. 44,023
Patent Attorney
Intel Americas, Inc.
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026